DICOM®

Digital Imaging and Communications in Medicine

September 12, 2019

Pia Dangelmayer
Bayerischer Rundfunk
[redacted]

Dear Pia Dangelmayer:

DICOM is taking the opportunity you offered to provide its thoughts on your analysis regarding the security of medical image data managed by others. Much has already been achieved to make medical data more secure. Still, additional effort is helpful to educate more broadly those charged with applying the proper measures for keeping data secure.

Dr. Pianykh's study implies that some sites with DICOM-capable systems may need to better address security issues, for example, by using established DICOM Secure Communications Profiles and Audit logs, as documented in the Integrating the Healthcare Enterprise (IHE) ATNA profile (https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication).

Your assertion that there are "millions of sensitive datasets on patients" at risk, if based solely on Dr. Pianykh's research, is not valid. Unless he did follow-up research, his published paper does not confirm that those systems have any sensitive data on them. Further, it does not make any assertions about the numbers of datasets or that those systems would release any sensitive data if requested. He simply identified systems that would respond to a DICOM Association Negotiation request by accepting such a request (~700) or by rejecting it (~2000), and he apparently did not attempt to discover what was on those systems. Entries in the Shodan database (https://www.shodan.io/) indicate a variety of types of DICOM-capable systems (e.g., viewers) responding to connections, not just PACS servers. For instance, recent interest in artificial intelligence processing of medical images has resulted in contests where research data (very large numbers of medical images which have been scrubbed of patient identifying information) is posted on public servers for contestants use in developing and testing their algorithms. Without close inspection, these DICOM images might appear to be private patient data.

This is not to suggest that situations don't exist where patient data could be exposed, or that hospitals and other medical imaging facilities have no further room for improvement. Rather, this situation is complex, and inferences based on numerical estimates should be made with great caution.

DICOM response to specific questions

1. Do you know of the problem that millions of datasets of patients are openly accessible on the internet?

No. We are aware there are about 700 to 800 systems that will respond to an ordinary connection request for DICOM services over the open internet. We know this includes test systems provided by vendors, educational systems for use by students, archives of educational material, veterinary hospital systems, and materials testing labs (DICOM is used for more than human medicine). We have not seen evidence that millions of datasets are openly accessible on the internet.

Due to concerns regarding the legality of exploring confidential databases, we do not know how one would go about arriving at an estimate of their own.

2. According to the minutes, Mr. Lawrence Tarbox was tasked to reach out to Mr. Pianykh and invite him to join WG-14. Did he ever extend that invitation and/or reach out? What was the result?

Dr. Tarbox was directed to the peer-reviewed journal article outlining Dr. Pianykh's research. The article sufficiently answered the questions that WG-14 had concerning the study.

3. According to the minutes, in November 2016, WG-14 was discussing whether "DICOM is perceived as a security risk (how serious is this, how true?)". After becoming aware of the study and Mr. Tarbox tasked with reaching out, the answer to this question seems to be yes, especially given that the publication of a follow-up research was being discussed in March 2017. Are we correct in assuming that WG-14 concludes that the findings of Mr. Pianykh are serious in nature and/or proof that DICOM indeed is to be judged as a security risk?

The statement in the minutes refers to perceptions which seem to exist in the market, as reflected in some media articles. The DICOM Standard Committee was most interested in how strongly and widely held these perceptions were and whether there might be some truth to them.

DICOM WG-14 concluded that the DICOM Standard did not inherently pose a security risk. The Secure Connection capability (specified in DICOM for almost two decades) is very secure. Proper security, however, requires more than just technical measures. It requires the implementation of institutional plans and policies to address various aspects of security (for example: infrastructure, device configuration, procedures, policies, training, auditing and oversight).

Papers like Dr. Pianykh's are useful to motivate healthcare providers and vendors to deploy the features that are available in DICOM. Security officers at hospitals prioritize their efforts based on the threats they observe and/or become aware of. Therefore, the work of Dr. Pianykh, Shodan and others is helpful in heightening security officers' awareness.

4. To the best of our knowledge, the DICOM standard committee didn't put out alerts or send out warnings to customers, and/or vendors, cloud infrastructure providers and hospitals that use these protocols and PACS-servers. Is that correct? If yes: Why didn't the DICOM standard committee put out warnings and/or alerts? If no: Can you send us copies of the warnings and/or alerts you put out?

WG-14 did not initiate a CVE report (an alert) because there did not seem to be any gap or abuse of the DICOM Standard specification involved. Security mechanisms are documented and there are legitimate needs for both open and secure connections.

It is not within the DICOM charter to examine all vendor products that implement all or some part of the DICOM Standard, or to evaluate customer installation, configuration, and use of those vendor products.

That said, the DICOM Standard Committee publicly published Part 15 (which is focused on the security-related mechanisms of the protocol) and notified the DICOM community (which includes vendors, users, governmental representatives and other interested parties) in 1999, and has publicly republished the standard many times since then.

5. Is security a traditional item in the scope of DICOM?

Yes, in terms of specifying security mechanisms in the DICOM Standard and making that information available to the DICOM community. The DICOM Standard Committee has considered security issues since its inception, ultimately leading to the formation of Working Group 14 on Security in the 1990s.

Starting in the late 1990s, WG-14 added security and privacy mechanisms to the DICOM protocol to support such things as secure network connections, digital signatures, encrypted email and media, encryption of files and parts of files, de-identification, audit trails, device authentication, and user identity-based access.

WG-14, the DICOM Standard Committee, and more recently WG-29 (Education, Communication, and Outreach) make a point of educating the DICOM community of the mechanisms available in the DICOM Standard. DICOM Security mechanisms are included in DICOM conference presentations on a regular basis and periodically in presentations at annual meetings of organizations such as the Radiological Society of North America (RSNA), Society for Imaging Informatics in Medicine, and American Association of Physicists in Medicine (AAPM). The DICOM website highlights security in the "Using DICOM" section (https://www.dicomstandard.org/using/security/). Members of WG-14, working as part of the Medical Imaging & Technology Alliance (MITA), prepared a series of security related whitepapers in a collaboration between MITA, COCIR, and the Japan Medical Imaging and Radiological Systems Industries Association (JIRA) from 2001-2007. (https://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/).

Properly securing an institution that might use the DICOM Standard goes well beyond the charter of DICOM and by extension, the responsibilities of its committee members. National Institute of Standards and Technology (NIST) and National Security Agency (NSA) documents make clear that a technical interchange standard by itself cannot assure security. It can provide the means to facilitate the secure exchange of information, but ultimately security is dependent on the environment in which the standard is used. If users do not deploy, activate and maintain secure communications protocols, or do not protect keys on which those protocols are based, there can be no guarantee of security.

6. If not, who is responsible for keeping PACS-servers safe and secure?

The actual implementation, deployment, purchase, maintenance and configuration of systems that implement the DICOM Standard are the responsibility of the product vendors and their customers. Further, it is the responsibility of the vendors to provide and maintain software implementations.

Some guidance on how a number of security topics can be collaboratively addressed is provided on the MITA website (https://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/)

Healthcare providers are regulated by the U.S. Department of Health and Human Services (HHS) and other agencies and are subject to rules such as Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Vendors are regulated by the U.S. Food and Drug Administration (FDA) and other agencies and are subject to regulatory cybersecurity directives.

DICOM is a standards development organization. Its responsibility is limited to defining and maintaining the standard so that it can be used effectively by vendors and institutions. The membership includes many manufacturers, medical professional societies, government organizations, and provider organizations.

7. Are there any cases you know of in which malicious actors were able to access this data?

No confirmed breaches due to flaws in the DICOM security protocol have been brought to the attention of the DICOM Standard Committee.

8. WG-14 was dormant for more than ten years. Right after the publication of Mr. Pianykh's study the working group comes back to life. Was the study of Mr. Pianykh the reason to re-establish WG-14? If not: Why was this group dormant for more than ten years and why was it re-established?

WG-14 was extremely active in the late 1990s and early 2000s, publishing seven major supplements to the DICOM Standard covering technical capabilities that could be incorporated into vendor products and used by provider sites to enhance security. These mostly leveraged general IT standards, such as Transport Layer Security (TLS) (the same protocol that secures web transactions). By 2006, the planned objectives of WG-14 were completed and the group's focus turned to maintenance of the specifications. WG-14 continued to report at meetings of the DICOM Standard Committee, keeping abreast of developments and monitoring for potential additional work items. In 2015, independent of Dr. Pianykh's work, WG-14 launched several new work items aimed at improvements to some mechanisms already in the Standard, retiring some mechanisms that were obsolete, and evaluating whether any new mechanisms were needed to support the new DICOMweb™ protocols. Dr. Pianykh's concerns came to our attention while these activities progressed.

Important Points to Consider

1. ***DICOM added a secure connection capability to the standard in 1999, 20 years ago.***

   Prior to 1999, products assumed they were being run on a secured (e.g. limited access) network.

2. ***DICOM specifies protocols; vendors implement those protocols in their products' features; healthcare providers install and operate those products, utilizing those features.***

   DICOM is responsible for defining relevant security mechanisms in our protocol. Vendors are responsible for implementing security features in their products. Healthcare providers are responsible for securing their facility and making appropriate use of security features.

3. ***We estimate there are about a million DICOM-capable devices in the world; the vast majority of those have been installed and configured with some degree of security.***

   The Shodan database identifies ~700 systems in the US that have been installed and configured with an open connection on the public internet, which agrees with Dr. Piankyh's experiments. Even though it is a comparatively small number, it may be possible that some of those systems may contain patient records. Those likely represent bad configuration choices on the part of those operating those systems. Some of those 700 systems do not contain patient records and have open connections to support product development, product demonstration, interoperability testing, product evaluations or performance tests, anonymized education or research datasets, and veterinary data.

If you have any questions, please do not hesitate to email or call.

Kind regards,

Lisa Spellman
DICOM General Secretary

[redacted]

Secretariat:
1300 North 17th Street, Suite 900
Arlington, VA 22209, USA
http://dicom.nema.org
dicom@medicalimaging.org
+1-703-841-3259

Minutes-tcon

DICOM WORKING GROUP 14

(Security)

March 15, 2017

Voting Members Present	**Represented by**
ACR	James Philbin
Agfa Healthcare	Rob Horn
JIRA	Akihiro Yomoda
N/A	John Moehrke
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox

Voting Members Not Present	**Represented by**
FUJIFILM Medical Systems	Masao Murata
GE Healthcare	Francisco Sureda
Laitek	Doug Sluis
OFFIS	Marco Eichelberg
PixelMed	David Clunie
Philips Healthcare	Ben Kokx
Siemens	Hans-Martin Von Stockhausen
Stryker Communications	Corey Cochran

Alternate Voting Members, Observers, Guests Present	
MITA/DICOM Secretariat	Cheryl Kreider Carey
MITA/DICOM Secretariat	Luiza Kowalczyk

Presiding Officers	Lawrence Tarbox, User Co-Chair Rob Horn, Industry Co-Chair
DICOM Secretary	Cheryl Kreider Carey

1. **Opening**

   The meeting was called to order at 9.10 am USA Eastern Time. The Secretary reviewed the antitrust rules. The Agenda was approved. Minutes from February 21, 2017 were approved as amended (acronym for ATNA was corrected).

2. **CP's**

   Confirmed that there were no CP's.

3. **Work Item Proposal for DICOMweb Security DRAFT**

   Version 2 of Work Item Proposal for DICOMweb Security was discussed, specifically whether any additional information was needed.

   Action: Cheryl to submit WIP v.2 for approval at DSC at April 2017 meeting in Romania (invite by telephone)

   Question for DSC: should this WIP be accelerated?

4. **Discussion on Article and Original research published in AJR**

   "Unprotected DICOM servers remain a security risk" written by Erik L. Ridley, Aunt Minnie staff writer: http://www.auntminnie.com/index.aspx?sec=ser&sub=def&pag=dis&ItemID=116258

   Rather than DICOM writing a letter to the editor of AJCR/American Journal of Cancer Research as originally agreed, discussion included meeting with author of research to explore ways to help with follow-up research article. MITA/MII Section should address security with FDA.

   Action:

   - Lawrence to invite author of AJCR article to present findings to WG-14, with potential follow-up research and article. Invite WG-06 and WG-23 to join presentation, as well as MITA's Medical Imaging Informatics (MII) Section chair and staff delegate.

5. **New Business**

6. **Next Meetings**

   T-con

   - Wednesday, April 19, 09:00-10:00 USA Eastern Time
   - Wednesday, May 17, 09:00-10:00 USA Eastern Time

   In person

   - Not scheduled yet

7. **Adjournment**

   The meeting was adjourned at 10:02 USA Central Time.

   Reported Cheryl Kreider Carey, DICOM, Secretary
   Reviewed by Clark Silcox, Legal Counsel, CRS

Secretariat:
1300 North 17th Street, Suite 900
Arlington, VA 22209, USA
http://dicom.nema.org
dicom@medicalimaging.org
+1-703-841-3259

Minutes-tcon

WORKING GROUP 14

(Security)

April 19, 2017

Voting Members Present	**Represented by**
ACR	James Philbin
Agfa Healthcare	Rob Horn
Laitek	Doug Sluis
JIRA	Akihiro Yomoda
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox

Voting Members Not Present	**Represented by**
CMDS/CFDA	Jia Zheng
Change Healthcare	Roger Trevisan
Chiyoda Technol Corporation	Akihiro Yomoda
FUJIFILM Medical Systems	Masao Murata
Hologic	Jeff Garrett
GE Healthcare	Francisco Sureda
OFFIS	Marco Eichelberg
PixelMed	David Clunie
Philips Healthcare	Ben Kokx
Siemens	Hans-Martin Von Stockhausen
Stryker Communications	Corey Cochran

Alternate Voting Members, Observers, Guests Present	
Rogan-Delft BV	Pim Philipse
MITA/DICOM Secretariat	Cheryl Kreider Carey
MITA/DICOM Secretariat	Luiza Kowalczyk
N/A	John Moehrke

Presiding Officers	Lawrence Tarbox, User Co-Chair Rob Horn, Industry Co-Chair
DICOM Secretary	Cheryl Kreider Carey

1. Opening

The meeting was called to order at 9.05 am USA Eastern Time. The Secretary reviewed the antitrust rules. The Agenda was amended to include an update on Correction Proposals. Minutes from March 15, 2017 were reviewed.

2. Work Item Proposal: update from DICOM Standards Committee

Lawrence reported DSC had approved WG-14's DICOMweb Security Work Item Proposal the prior week at their spring meeting in Romania. Additionally, the DSC made no changes to the WIP. The only direction from DSC was for WG-14 to coordinate with MITA on any policy items related to security.

Next steps: Develop outline for "Security of DICOMweb Transactions" supplement

- Needed: An editor
- Target: August for draft to WG-06

Discussion included:

- Keep supplement flexible enough without blocking interoperability
- Since security isn't a traditional item in the scope of DICOM, we could point to IHE profiles rather than re-invent them
- IHE now recognized as standards development organization by ISO
- Provide education around the process: what you need to do, look at these alternatives, here are realistic ones, how to consider alternatives; don't give answer but explain how to describe the profiling
- Consider server side profile with encrypted channel (VLAN, traditional TLS with server side only authentication); authentication from client side you go to different mechanism. Provide encryption but not client-side authentication**.** Describe a cafeteria style of options, with lowest common denominator to ensure interoperability
- DICOM audience would love Part 17 illustrious walk through of all decisions to make for web OAuth for deployment, describe the process; there isn't a book within security that describes this process, thus writing down the process would add value.

Action: Lawrence will draft outline of supplement with laundry list, e.g. single side TLS, OAuth 2 web based access

3. Correction Proposals

Rob presented two (2) Correction Proposals assigned to him. These two CP's will be reviewed at WG-06 June meeting:

- CP-1703 --TLS Security Note for Web Services.
- CP-1353 -- Secure Transport Connection Profile should allow higher TLS versions.

4. **Original researcher published in AJCR,** highlighted in "Unprotected DICOM servers remain a security risk" in Aunt Minnie.

   Lawrence acknowledged he still needs to follow through on his March 15 action item to invite the author of the research to a future WG-14 tcon. The group agreed Lawrence should proceed with extending the invite without a review by WG-14 first.

   Action: Lawrence to invite author of AJCR article to present findings to WG-14, with potential follow-up research and article. Invite WG-06 and WG-23 to join presentation, as well as MITA's Medical Imaging Informatics (MII) Section chair and staff delegate.

5. **New Business**

6. **Next Meetings**

   T-con: 3rd Wednesday's of month
   - Wednesday, May 17, 09:00-10:00 USA ET
   - Wednesday, June 14, 09:00-10:00 USA ET (2nd Wed instead of to accommodate WG-06)

   In person
   - Not scheduled yet

7. **Adjournment**
   The meeting was adjourned at 10:02 USA Eastern Time.

   Reported by Cheryl Kreider Carey, DICOM, Secretary
   Reviewed by Clark Silcox, Legal Counsel

Secretariat:
1300 North 17th Street, Suite 900
Arlington, VA 22209, USA
http://dicom.nema.org
dicom@medicalimaging.org
+1-703-841-3259

Minutes-tcon

WORKING GROUP 14

(Security)

May 17, 2017

Voting Members Present	**Represented by**
ACR	James Philbin
Agfa Healthcare	Rob Horn
Chiyoda Technol Corporation/JIRA	Akihiro Yomoda
Laitek	Doug Sluis
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox

Voting Members Not Present	**Represented by**
CMDS/CFDA	Jia Zheng
Change Healthcare	Roger Trevisan
FUJIFILM Medical Systems	Masao Murata
Hologic	Jeff Garrett
GE Healthcare	Francisco Sureda
OFFIS	Marco Eichelberg
PixelMed	David Clunie
Philips Healthcare	Ben Kokx
Siemens	Hans-Martin Von Stockhausen
Stryker Communications	Corey Cochran

Alternate Voting Members, Observers, Guests Present	
JIRA	Shinichi Nakano
JIRA	Takashi Igarashi
N/A	John Moehrke
Rogan-Delft BV	Pim Philipse
MITA/DICOM Secretariat	Cheryl Kreider Carey
MITA/DICOM Secretariat	Luiza Kowalczyk

Presiding Officers	Lawrence Tarbox, User Co-Chair Rob Horn, Industry Co-Chair
DICOM Secretary	Cheryl Kreider Carey

1. **Opening**

   The meeting was called to order at 9.03 am USA Eastern Time. The Secretary reviewed the antitrust rules. Minutes from April 19, 2017 were approved.

2. **FDA Public Workshop – Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis, May 18-19, 2017**
   Rob is attending FDA's workshop on cybersecurity this week as an Agfa rep but offered to relay any input from WG-14. The purpose of the workshop is to look for regulatory gaps. Rob said a motivation for the workshop was the St. Jude incident, where a cardiac monitor had various security flaws that went into their tracking system, but concluded it was an insignificant risk not worth addressing.

Action Item #1: WG-14 to review FDA cybersecurity agenda and forward any items you'd like addressed at the workshop to Cheryl by 8amET May 18.

3. **Draft outline for "Security of DICOMweb Transactions" supplement**
   Due to extenuating circumstances, Lawrence was unable to complete the two actions items from April meeting to draft outline of the supplement and to invite AJCR author to tcon. Discussion included:

   - Include ATNA profile in supplement versus CP. Not making technology change, just raising visibility of technology that's already there. Profile that's bi-directional and uni-directional authentication.
   - Willingness to have DICOM point to IHE where appropriate rather than duplicating same text, e.g. security
   - Point at clinical recommendations. Don't include them but reference "this information is useful for that" and reference paper from AAPM.
   - Profiles to be required: three from secure transport files, two using TLS.
   - ISCL transfer profile and TLS: question for our Japanese colleagues, is ISCL still used or should it be retired?

Action Item #2: Lawrence to draft inquiry to JIRA regarding use of ISCL; will send draft to group before forwarding to JIRA.

- Informative Annex in Part 17: if you decide to use open connect, here's how it would work
- Connection profiles in scope; Audit trail out of scope
- Look at Digital Signature Profiles

Action Item #3: Lawrence to draft outline of supplement: tweak sections of Part 15 to make applicable to web case as well as DIMSE case and focus on Part 17 with expanded policy.

Action Item #4 (from April): Lawrence to invite author of AJCR article to present findings to WG-14, with potential follow-up research and article. Invite WG-06 and WG-23 to join presentation, as well as MITA's Medical Imaging Informatics (MII) Section chair and staff delegate.

4. **New Business**

5. **Next Meetings**

T-con: 3rd Wednesday's of month

- Wednesday, June 14, 09:00-10:00 USA ET (2nd Wed instead of to accommodate WG-06)

In person

- Not scheduled yet

6. **Adjournment**

The meeting was adjourned at 9:55 USA Eastern Time.

Reported by Cheryl Kreider Carey, DICOM, Secretary
Reviewed by Clark Silcox

Secretariat:
1300 North 17th Street, Suite 900
Arlington, VA 22209, USA
http://dicom.nema.org
dicom@medicalimaging.org
+1-703-841-3259

Minutes-tcon

WORKING GROUP 14

(Security)

June 14, 2017

Voting Members Present	**Represented by**
Agfa Healthcare	Rob Horn
Chiyoda Technol Corporation/JIRA	Akihiro Yomoda
FUJIFILM Medical Systems	Masao Murata
Siemens	Hans-Martin Von Stockhausen
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox

Voting Members Not Present	**Represented by**
ACR	James Philbin
CMDS/CFDA	Jia Zheng
Change Healthcare	Roger Trevisan
Hologic	Jeff Garrett
GE Healthcare	Francisco Sureda
Laitek	Doug Sluis
OFFIS	Marco Eichelberg
PixelMed	David Clunie
Philips Healthcare	Ben Kokx
Stryker Communications	Corey Cochran

Alternate Voting Members, Observers, Guests Present	
JIRA	Takashi Igarashi
Rogan-Delft BV	Pim Philipse
MITA/DICOM Secretariat	Cheryl Kreider Carey
VA	John Moehrke

Presiding Officers	Lawrence Tarbox, User Co-Chair Rob Horn, Industry Co-Chair
DICOM Secretary	Cheryl Kreider Carey

1. **Opening**

The meeting was called to order at 9.05 USA Eastern Time. The Secretary reviewed the antitrust rules. The Agenda was amended to add an update on the FDA Cybersecurity Forum from Rob Horn. Minutes from May 17, 2017 were approved.

2. **Administrative**

Following the pattern of third Wednesday of month, from 9.00-10.00 USA ET, future calls of WG-14 were determined: July 19, Aug 16, Sep 20, Oct 18, and Nov 15. Invitation will be sent.

3. **FDA Public Workshop: Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis**

Rob Horn highlighting the following from the FDA's Cyber workshop held May 18-19, 2017:

- Security – CIA: Confidentiality-Integrity-Availability
  - Confidentiality is not a problem; Integrity is a major problem area; Availability is major problem area
  - FDA will be emphasizing that security includes integrity and availability, not just confidentiality.
- Threat Models – How are threats evolving and changing? How do different threat models affect the sharing of responsibility between healthcare delivery organizations (HDO) and device manufacturers?
- SBoM—Software Bill of Materials (very misleading name). Use cases need to be created. SBoM needs to be usable, not complete. What level of detail is appropriate? HDO needs a "software BoM" to prioritize response.
- Validation and Verification under time pressure:
  - What design changes will address the mismatch between software life cycles (3-7 years) and device capital desires (10-30 years)?
  - Discussions admired the problem without having a ready general solution. FDA is listening.
- **WannaCry postmortem: ISAO did not solve coordination problem. Healthcare-ISAC, FDA, HHS, and DHS all ran parallel redundant coordinating efforts.**
- Next steps: Rob believes the FDA:
  - Will work on balancing C-I-A since it doesn't take regulation.
  - Will need to do something with Threat Model but not sure when
  - Continue talking about SBoM but not ready for regulation; more academic work
  - Gets the issue with Validation and Verification (didn't get it last time) but don't know how to respond, like manufacturers.

Action Item: Rob to post slides to meeting folder, if permission is granted.

4. **CP Update: CP-1616**

Rob explained some descriptive material found in RFC3881 did not get moved into the descriptive table.

5. **Draft outline for "Security of DICOMweb Transactions" supplement**

Larry reviewed outline and asked for volunteers to write a section:

Part 2 –
Part 15 –Pim Philipse
Part 17 –
Part 18 -

6. **Old Business**

Action Item #4 (from April): Lawrence to invite author of AJCR article to present findings to WG-14, with potential follow-up research and article. Invite WG-06 and WG-23 to join presentation, as well as MITA's Medical Imaging Informatics (MII) Section chair and staff delegate.

7. **New Business**

8. **Next Meetings**

T-con: 3rd Wednesday's of month

- Wednesday, July 19, 09:00-10:00 USA ET
- Wednesday, August 16, 09:00-10:00 USA ET
- Wednesday, October 18, 09:00-10:00 USA ET
- Wednesday, November 15, 09:00-10:00 USA ET

In person

- Not scheduled yet

9. **Adjournment**

The meeting was adjourned at 10.06 USA Eastern Time.

Reported by Cheryl Kreider Carey, DICOM, Secretary
Reviewed by : Clark Silcox

Secretariat:
1300 North 17th Street, Suite 900
Arlington, VA 22209, USA
http://dicom.nema.org
dicom@medicalimaging.org
+1-703-841-3259

Minutes-tcon

WORKING GROUP 14

(Security)

July 19, 2017

Voting Members Present	**Represented by**
Agfa Healthcare	Rob Horn
Change Healthcare	Roger Trevisan
PixelMed	David Clunie
Philips Healthcare	Ben Kokx
Siemens	Niki Wirsz
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox

Voting Members Not Present	**Represented by**
ACR	James Philbin
Chiyoda Technol Corporation/JIRA	Akihiro Yomoda
CMDS/CFDA	Jia Zheng
Change Healthcare	Roger Trevisan
FUJIFILM Medical Systems	Masao Murata
Hologic	Jeff Garrett
GE Healthcare	Francisco Sureda
Laitek	Doug Sluis
OFFIS	Marco Eichelberg
Stryker Communications	Corey Cochran

Alternate Voting Members, Observers, Guests Present	
JIRA	Takashi Igarashi
MITA/DICOM Secretariat	Cheryl Kreider Carey

Presiding Officers	Lawrence Tarbox, User Co-Chair Rob Horn, Industry Co-Chair
DICOM Secretary	Cheryl Kreider Carey

1. **Opening**

The meeting was called to order at 9.05 USA Eastern Time. The Secretary reviewed the antitrust rules. The Agenda was approved. Minutes from June 14, 2017 were approved.

2. **Administrative**

- Following discussion, the decision was for WG-14 to not meet in-person during RSNA 2017. Rather, WG-14 will meet by tcon on November 15 at 09.00 USA ET as originally scheduled.
- Note: if anyone speaks with Oleg Pianykh, PhD, of Massachusetts General Hospital (MGH) during RSNA 2017, notify him that WG-14 would like to invite him to participate in WG-14 and refer him to Larry Tarbox. Note: Oleg presented findings during RSNA 2016 that were also published in AJCR.

3. **Draft outline and assignments: *Security of DICOMweb Transactions***

Larry reviewed outline and asked for volunteers to write a section. Current authors included:

Part 2 –

Part 15 – revise and modernize - Pim Philipse

- Review existing profiles for any needed changes, possibly retiring antique profiles – Rob Horn
  - Profile on RFC 7525, best practices for TLS – Rob Horn
  - Possibly retiring antique profiles
- Add profile or revise existing profiles to support secure communications for DIOCM RESTful services
- Consider one or more profiles for user/role authentication, possibly referring to IHE XUA

Part 17 –

- Review existing examples and revise as needed
- Add new examples illustrating good security practices for web-based DICOM protocols – Lawrence Tarbox
- Add examples of use/role authentication, and how it ties to authorization
  - Directly with DIMSE service providers – Lawrence Tarbox
  - With a thin server intermediary that translates from RESTful to DIMSE – Lawrence Tarbox
  - With a full RESTful server implementation – Lawrence Tarbox
  - Swiss work on delegated authority on access—access control question to a regional server – Rob Horn
  - In connection with SMART on FHIR, E.g. SMART on RESTful DICOM (not standard) – Rob Horn
- Consider other examples deemed appropriate, e.g. crossing DIMSE and web based protocol boundaries

Part 18 -

- Review, revise if needed to clarify security issues, possibly referring back to profiles in Part 15

- Action Item (from April): Lawrence to invite author of AJCR article to present findings to WG-14, with potential follow-up research and article. Invite WG-06 and WG-23 to join presentation, as well as MITA's Medical Imaging Informatics (MII) Section chair and staff delegate.

4. Next Meetings

T-con: 3rd Wednesday's of month

- August 16, 09:00-10:00 USA ET
- September 20, 09:00-10:00 USA ET
- October 18, 09:00-10:00 USA ET
- November 15, 09:00-10:00 USA ET

In person

- Not scheduled yet

5. Adjournment

The meeting was adjourned at 9.41 USA Eastern Time.

Reported by Cheryl Kreider Carey, DICOM, Secretary
Reviewed by: Clark Silcox

Secretariat:
1300 North 17th Street, Suite 900
Arlington, VA 22209, USA
http://dicom.nema.org
dicom@medicalimaging.org
+1-703-841-3259

Minutes-tcon

WORKING GROUP 14

(Security)

August 16, 2017

Voting Members Present	**Represented by**
Agfa Healthcare	Rob Horn
FUJIFILM Medical Systems	Masao Murata
Philips Healthcare	Ben Kokx
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox

Voting Members Not Present	**Represented by**
ACR	James Philbin
Change Healthcare	Roger Trevisan
PixelMed	David Clunie
Chiyoda Technol Corporation/JIRA	Akihiro Yomoda
CMDS/CFDA	Jia Zheng
Change Healthcare	Roger Trevisan
Hologic	Jeff Garrett
GE Healthcare	Francisco Sureda
Laitek	Doug Sluis
OFFIS	Marco Eichelberg
Siemens	Niki Wirsz
Stryker Communications	Corey Cochran

Alternate Voting Members, Observers, Guests Present	
JIRA	Takashi Igarashi
NA	John Moehrke
Rogan-Delf BV	Pim Philipse
MITA/DICOM Secretariat	Cheryl Kreider Carey

Presiding Officers	Lawrence Tarbox, User Co-Chair Rob Horn, Industry Co-Chair
DICOM Secretary	Cheryl Kreider Carey

1. **Opening**

The meeting was called to order at 9.05 USA Eastern Time. The Secretary reviewed the antitrust rules. The Agenda was approved. Minutes from July 19, 2017 were approved.

2. **Reviewed assignments for *Security of DICOMweb Transactions***

Discussion focused on Part 15:

a) Rob Horn presented CP-1353 which WG-06 had reviewed in June/Iceland: *Secure Transport Connection Profile should allow higher TLS versions*. Following discussion, our recommendation will be to:
   - Retire: Basic TLS
   - Rename AES-TLS: Best Current Practice TLS with revisions
     - Exists to maintain legacy support , BCP 195 rationale
     - Shall comply with the RFC
   - Add: Best Current Practice "with restrictions"
     - Modifies requirements in RFC

WG-6 will discuss whether it goes through as CP or a supplement

b) Pim Philipse: discussion regarding other profiles to modernize
   - Go through existing profiles in Annex B, C, and D and determine what to do with them
   - Web-based DICOM protocols

Action Item: Homework assignments for ***Security of DICOMweb Transactions:***

Part 17 –

- Review existing examples and revise as needed
- Add new examples illustrating good security practices for web-based DICOM protocols – Lawrence Tarbox
- Add examples of use/role authentication, and how it ties to authorization
  - Directly with DIMSE service providers – Lawrence Tarbox
  - With a thin server intermediary that translates from RESTful to DIMSE – Lawrence Tarbox
  - With a full RESTful server implementation – Lawrence Tarbox
  - Swiss work on delegated authority on access—access control question to a regional server – Rob Horn
  - In connection with SMART on FHIR, E.g. SMART on RESTful DICOM (not standard) – Rob Horn
- Consider other examples deemed appropriate, e.g. crossing DIMSE and web based protocol boundaries

Part 18 -

- Review, revise if needed to clarify security issues, possibly referring back to profiles in Part 15

- Action Item (from April): Lawrence to invite author of AJCR article to present findings to WG-14, with potential follow-up research and article. Invite WG-06 and WG-23 to join presentation, as well as MITA's Medical Imaging Informatics (MII) Section chair and staff delegate.

c) Next Meetings

T-con: 3rd Wednesday's of month

- September 20, 09:00-10:00 USA ET
- October 18, 09:00-10:00 USA ET
- November 15, 09:00-10:00 USA ET

In person

- Not scheduled yet

d) Adjournment

The meeting was adjourned at 10.0 USA Eastern Time.

Reported by Cheryl Kreider Carey, DICOM, Secretary
Reviewed by: Clark Silcox